METHOD AND PROGRAM FOR AUTOMATICALLY PROCESSING ANNOYING MAIL IN MAIL SERVER OF MOBILE PHONE

Patent number: JP2003249964
Publication date: 2003-09-05
Inventor: SHIRATO HIROYUKI
Applicant: NEC COMMUNICATION SYST
Classification:
- international: ***G06F13/00; H04L12/58;*** **G06F13/00; H04L12/58;** (IPC1-7): H04L12/58; G06F13/00
- european:
Application number: JP20020046836 20020222
Priority number(s): JP20020046836 20020222

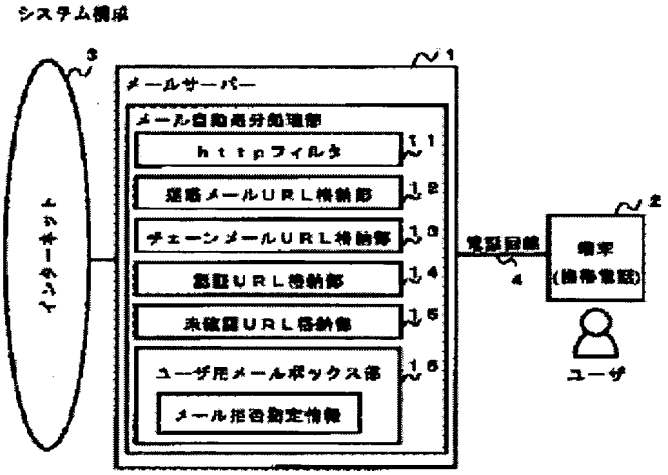
Report a data error here

Abstract of **JP2003249964**

PROBLEM TO BE SOLVED: To automatically discriminating annoying mails or the like in a mail server of a mobile phone by a prescribed discrimination condition to prevent unnecessary reception by automatic deletion and to allow a user to utilize a system by easy user's setting.

SOLUTION: The mail server of the mobile phone has a step wherein it is checked whether a URL is included in the mail text of a mail received through a network or not and the URL is extracted when included, a step wherein the extracted URL is used to discriminate whether the received mail is an annoying mail or a chain mail, and a step wherein the received mail discriminated as an annoying mail or a chain mail as a result of discrimination is not stored in a mail box for the user and is deleted. The discrimination condition is automatically updated at any time.

COPYRIGHT: (C)2003,JPO



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開2003－249964

（P2003－249964A）

(43)公開日　平成15年９月５日(2003.9.5)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｈ０４Ｌ　12/58	１００	Ｈ０４Ｌ　12/58	１００Ｆ　５Ｋ０３０
Ｇ０６Ｆ　13/00	６１０	Ｇ０６Ｆ　13/00	６１０Ｑ

審査請求　未請求　請求項の数20　ＯＬ　（全 15 頁）

(21)出願番号　特願2002－46836(P2002－46836)

(22)出願日　平成14年２月22日(2002.2.22)

(71)出願人　000232254
日本電気通信システム株式会社
東京都港区三田１丁目４番28号
(72)発明者　白戸　寛之
東京都港区三田一丁目４番28号　日本電気通信システム株式会社内
(74)代理人　100084250
弁理士　丸山　隆夫

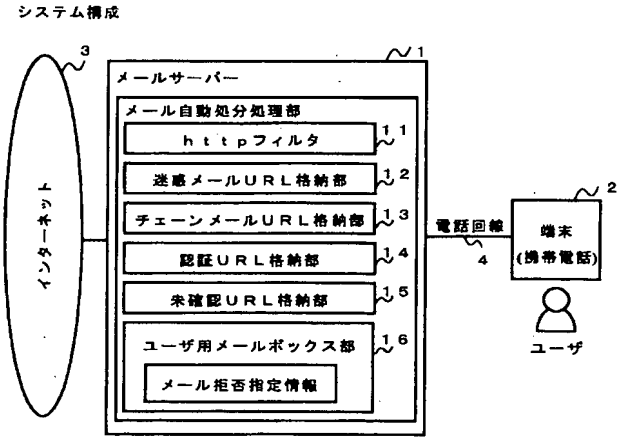
Ｆターム(参考)　5K030 GA11 HA06 LC15

(54)【発明の名称】　携帯電話のメールサーバーにおける迷惑メール自動処分方法及びプログラム

(57)【要約】

【課題】　携帯電話のメールサーバーにおいて所定の識別条件により迷惑メール等を自動的に識別し、自動削除処理を行って余計な受信を防止すること。また、簡単なユーザ設定によりシステムを利用可能とすること。

【解決手段】　携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にＵＲＬが含まれるかどうかを調べ、含まれる場合は抽出する工程と、抽出されたＵＲＬを用いて受信メールが迷惑メールあるいはチェーンメールであるかの識別処理を行う工程と、識別処理の結果、迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除処理する工程とを有する。上記識別条件は随時自動更新される。



1

【特許請求の範囲】

【請求項１】　携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、
メール本文中にＵＲＬが含まれるかどうかを調べ、含まれる場合は抽出する抽出工程と、
該工程で抽出されたＵＲＬに基づき前記受信メールが迷惑メールあるいはチェーンメールであるか否かの識別処理を行う識別工程と、
該工程で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除処理する削除工程と、を有することを特徴とする迷惑メール自動処分方法。

【請求項２】　前記識別工程で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれていたＵＲＬを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する工程をさらに有することを特徴とする請求項１記載の迷惑メール自動処分方法。

【請求項３】　前記抽出工程で抽出されたＵＲＬが未確認ＵＲＬである場合、該未確認ＵＲＬを本文中に含む受信メールに対する所定時間の監視処理を開始し、該所定時間内は前記未確認ＵＲＬを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、前記所定時間経過後、前記受信件数が所定件数を超える場合、前記未確認ＵＲＬを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する監視工程をさらに有することを特徴とする請求項１または２に記載の迷惑メール自動処分方法。

【請求項４】　前記監視工程において、前記一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、前記未確認ＵＲＬを本文中に含むメールは迷惑メールであると判定する工程をさらに有することを特徴とする請求項３記載の迷惑メール自動処分方法。

【請求項５】　前記監視工程において、前記一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、前記未確認ＵＲＬを本文中に含むメールはチェーンメールであると判定する工程をさらに有することを特徴とする請求項３記載の迷惑メール自動処分方法。

【請求項６】　前記監視工程の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたＵＲＬを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する工程をさらに有することを特徴とする請求項３から５のいずれか１項に記載の迷惑メール自動処分方法。

【請求項７】　前記メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたＵＲＬを前記識別処理の際の識別条件となるＵＲＬ情報として登録して管理し、
前記識別工程では、

2

前記抽出工程で抽出されたＵＲＬについて、前記ＵＲＬ情報と比較し、一致する場合、前記受信メールを迷惑メールあるいはチェーンメールであると識別することを特徴とする請求項１から６のいずれか１項に記載の迷惑メール自動処分方法。

【請求項８】　前記メールサーバーにおいて、ユーザ設定情報として、前記識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、
前記受信メールについて迷惑メールあるいはチェーンメールと識別した場合、前記メール拒否指定の設定に基づき前記削除処理を実行することを特徴とする請求項１から７のいずれか１項に記載の迷惑メール自動処分方法。

【請求項９】　前記メールサーバーにおいて、前記メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、ＵＲＬを本文中に含むメールに対する拒否指定であるＵＲＬメール拒否指定の３つの設定を保持し、該設定に基づき前記削除処理を実行することを特徴とする請求項８記載の迷惑メール自動処分方法。

【請求項１０】　前記メールサーバーは、該メールサーバーの管理者により認証を受けたＵＲＬを登録して管理し、該ＵＲＬを本文中に含む受信メールについては前記迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する工程を有することを特徴とする請求項１から９のいずれか１項に記載の迷惑メール自動処分方法。

【請求項１１】　携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、
メール本文中にＵＲＬが含まれるかどうかを調べ、含まれる場合は抽出する抽出処理と、
該処理で抽出されたＵＲＬに基づき前記受信メールが迷惑メールあるいはチェーンメールであるか否かを識別する識別処理と、
該処理で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除する削除処理と、をコンピュータに実行させることを特徴とする迷惑メール自動処分プログラム。

【請求項１２】　前記識別処理で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれるＵＲＬを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する処理をさらにコンピュータに実行させることを特徴とする請求項１１記載の迷惑メール自動処分プログラム。

【請求項１３】　前記抽出工程で抽出されたＵＲＬが未確認ＵＲＬである場合、該未確認ＵＲＬを本文中に含む受信メールに対する所定時間の監視処理を開始し、該所定時間内は、前記未確認ＵＲＬを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、前

記所定時間経過後、前記受信件数が所定件数を超える場合、前記未確認ＵＲＬを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する処理をコンピュータに実行させることを特徴とする請求項１１または１２に記載の迷惑メール自動処分プログラム。

【請求項１４】　前記監視処理において、前記一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、前記未確認ＵＲＬを含むメールは迷惑メールであると判定する処理をコンピュータに実行させることを特徴とする請求項１３記載の迷惑メール自動処分プログラム。

【請求項１５】　前記監視処理において、前記一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、前記未確認ＵＲＬを含むメールはチェーンメールであると判定する処理をコンピュータに実行させることを特徴とする請求項１３記載の迷惑メール自動処分プログラム。

【請求項１６】　前記監視処理の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたＵＲＬを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する処理をコンピュータに実行させることを特徴とする請求項１３から１５のいずれか１項に記載の迷惑メール自動処分プログラム。

【請求項１７】　前記メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたＵＲＬを前記識別処理の際の識別条件となるＵＲＬ情報として登録して管理し、

前記識別処理では、

前記抽出処理で抽出されたＵＲＬについて、前記ＵＲＬ情報と比較し、一致する場合、前記受信メールを迷惑メールあるいはチェーンメールであると識別する処理をコンピュータに実行させることを特徴とする請求項１１から１６のいずれか１項に記載の迷惑メール自動処分プログラム。

【請求項１８】　前記メールサーバーにおいて、ユーザ設定情報として、前記識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、

前記受信メールについて迷惑メールあるいはチェーンメールと識別した場合、前記メール拒否指定の設定に基づき前記削除処理を行う処理をコンピュータに実行させることを特徴とする請求項１１から１７のいずれか１項に記載の迷惑メール自動処分プログラム。

【請求項１９】　前記メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、ＵＲＬを本文中に含むメールに対する拒否指定であるＵＲＬメール拒否指定の３つの設定を保持し、該設定に基づき前記削除処理を行う処理をコンピュータに実行させることを特徴とする請求項１８記載の迷惑メール自動処分プログラム。

【請求項２０】　前記メールサーバーにおいて、該メールサーバーの管理者により認証を受けたＵＲＬを登録管理し、該ＵＲＬを本文中に含む受信メールについては前記迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する処理をコンピュータに実行させることを特徴とする請求項１１から１９のいずれか１項に記載の迷惑メール自動処分プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯電話における電子メール技術に関し、特に、携帯電話のメールサーバーにおいて迷惑メール等を削除するメール自動処分方法及びプログラムに関する。

【０００２】

【従来の技術】昨今の電子メール機能を備える携帯電話機においては、迷惑メールによる被害が大きな問題になっている。被害として、ユーザの不快感や不要なパケット料金の支払いによる被害等が挙げられる。迷惑メールとしては様々な形態があり得るが、例えば、同一送信者からの大量のメールや、異なる送信者から同時に送信されてくるメール（チェーンメール）、あるいは、望まない広告や勧誘のメールなどがある。このようなメールに対する対策として、何らかの方法によりメールを自動的に排除・処分するシステムが求められている。

【０００３】従来の迷惑メール自動処分システムの一例として、特開２０００－１６３３４１号公報に開示されている技術がある。以下、この技術を例に採って従来技術について説明する。図１０は、この従来技術について説明するためのシステム構成図である。インターネット３には複数のメールサーバー１が接続されている。メールサーバー１には、電話回線４を通じて電子メール利用者（以下、ユーザ）の端末（携帯電話機）２が複数接続される。端末２は、電子メールの作成及び送受信機能を備える。電子メール（以下、「メール」）は、インターネット３を介してメールサーバー１間で送受信（配送、転送）処理される。メールサーバー１は、所定のメールサーバーソフトウェア（プログラム）を備える。

【０００４】メールサーバー１の各々は、個々のユーザに対するメール受信条件情報５を保持している。図１１は、従来システムにおけるメールサーバー１での迷惑メール自動処分処理において用いられるメール受信条件情報５の構成図である。図１１で、メール受信条件情報５には、ユーザのメール受信条件として、同一送信者条件５１、最大サイズ条件５２、既知送信者リスト５３の情報が記述されている。

【０００５】同一送信者条件５１は、同一のメール送信者から受信可能な（受信許可する）１日当たりのメール件数の上限値（例えば図１０では、１０件／日＝１日当たり１０件まで）を表しており、同一のメール送信者から１日に大量の件数のメールを受信することを制限する

ために用いられる。

【０００６】最大サイズ条件５２は、メール１件当たりの受信可能なデータ量の上限値（例えば図１０では、５００ＫＢ／件＝１件当たり５００ＫＢまで）を表しており、非常に大きなサイズのメールを受信することを制限するために用いられる。

【０００７】既知送信者リスト５３は、ユーザが既に知っている特定の個人（あるいはグループ）のメールアドレスが記述されるリストであり、ユーザが知らない個人（グループ）からのメール受信を制限するなどの目的で用いられる。例えば図１１では、”ａａａ＠ｘｘｘ．ｃｏ．ｊｐ”、”ｂｂｂ＠ｘｘｘ．ｃｏ．ｊｐ”等のメールアドレスがリストに登録されており、このアドレス情報を利用して受信メールについて所定の処理が行われる。

【０００８】メール受信条件情報５における以上の各項目は、ユーザが任意に設定できる。メールサーバー１は、メール受信者（ユーザ）毎に以下のようなメール自動削除設定情報６をメール受信条件情報５内に保持する。なお、ユーザはメールアドレスで区別される。メール自動削除設定情報６は、メール受信者（ユーザ）により設定されるメール送信者毎のメール自動削除処理に関する設定項目の一覧を保持する。図１２にメール自動削除設定情報６の構成を示す。

【０００９】このメール自動削除設定情報６として、メール送信者毎に、送信者メールアドレス６１、メール自動削除処理の対象とするか否かのオン／オフ設定６２、メール自動削除処理の対象とする場合の１日当たりの受信可能（受信許可）メール件数上限値（以下、「受信上限値」）６３、自動削除処理した場合に削除した旨の通知をメール送信者に対して行うか否かのオン／オフ設定（以下、「自動通知設定」）６４、を有する。

【００１０】また、ここで、メール送信者の要素に対する設定として、送信者不明メールについての設定６５、送信者未知メール（不明ではないが既知送信者リスト５３には記載されていない送信者からのメール）についての設定６６も行えるものとする。

【００１１】また、メール自動削除処理のための識別用の情報として、メール受信者（ユーザ）毎に、メール受信リスト６７、ある１日におけるメール送信者毎のメール受信件数６８を保持する。

【００１２】次に、上記従来システムの動作を説明する。図１３は、従来システムにおけるメールの送受信の様子を示す図である。例えば、同一のメール送信者７から、嫌がらせ等を目的とした大量のメールが送られてくる場合がある（俗にスパムメールと呼ばれる）。ただし、このようなメールの事例として、送信者メールアドレスが正規のものではない場合（ダミーのアドレスの場合）、あるいは、送信者メールアドレスが不明である場合なども含むとする。

【００１３】図１３で、メール送信者端末７からメールサーバー８を介して送出されるメールは、インターネット３を経由し、メール受信者（ユーザ）が利用するメールサーバー１に配送される。この際、メールサーバー１は、受信メールについて、ユーザにより予め設定されたメール受信条件情報５に基づき、この情報５内に記述されているメール受信条件を満足しないものを自動的に削除処理する。

【００１４】ここで、「メール受信条件を満足しない」とは、次の３つの条件のうち最低１つを満足することを指している。

１：送信されてきたメールの件数が、同一送信者条件５１で設定されている上限値を超えている。

２：送信されてきたメールのサイズが、最大サイズ条件５２で設定される上限値を超えている。

３：送信されてきたメールの送信者メールアドレスが、既知送信者リスト５３に記載されていない。

【００１５】メールサーバー１における受信メールのうち、メール受信条件情報５内のメール受信条件を満足するメールについては、そのままメールサーバー１内のメールボックスに蓄積される。ユーザが端末２を使用して電話回線４を介してメールサーバー１に接続されている状態において、メールサーバー１に蓄積されている該当ユーザ宛のメールが端末２へ送信される（＝端末２におけるメール受信の完了）。

【００１６】また、メールサーバー１は、メールを受信した際、受信メールから、メール受信者情報（宛先メールアドレス）、メール送信者情報（送信者メールアドレス）等を読む。続いて、該当メール受信者のメール自動削除設定情報６を参照しつつ、受信メールについて自動削除処理するか否かを識別・判定する。

【００１７】メール自動削除設定情報６に基づく識別の結果、受信メールを自動削除しない場合、ユーザのメールボックスに蓄積する。メール受信者（ユーザ）によるメールサーバー１へのアクセスなどにより、メールボックスに蓄積されているメールがユーザの端末２に送信される。一方、上記識別の結果、受信メールを自動削除する場合、そのメールの送信者が既知メール送信者リスト５３に記載されており、かつ自動通知設定６４が「通知する」に設定されているならば、自動削除した旨およびその理由などを記載したメールを削除されたメールのメール送信者７宛に自動送信する。

【００１８】次に、あるメール受信者（ユーザ）に関するメール自動削除設定情報６の例を説明する。例えば、不明送信者からのメールは１件たりとも受信しない設定にする場合、送信者メールアドレスが不明のメールに関して、自動削除機能６２を「有効（する）」に設定し、受信上限値６３を「０件」に設定し、自動通知機能６４を「無効（しない）」に設定する。

【００１９】また、未知送信者からのメールについて１

日当たり計２０件まで受信可能とする設定にする場合、送信者メールアドレスが未知であるメールに関して、自動削除機能６２を「有効」に設定し、受信上限値６３を「２０件」に設定し、自動通知機能６４を「有効」に設定する。

【００２０】また、送信者メールアドレスが”ａａａ＠ｘｘｘ．ｃｏ．ｊｐ”のメールは１日当たり３０件まで受信し、かつ自動削除した時に自動通知を行う設定にする場合、自動削除機能６２を「有効」に設定し、受信上限値６３を「３０件」に設定し、自動通知機能６４を「有効」に設定する。

【００２１】また、送信者メールアドレスが”ｂｂｂ＠ｘｘｘ．ｃｏ．ｊｐ”のメールは無制限に受信すると設定する場合、自動削除機能６２を「無効」に設定し、受信上限値６３を設定せず、自動通知機能６４を「無効」に設定する。以上の各設定は、図１４のようになる。

【００２２】次に、上記のように自動削除設定した場合での、あるメール受信者（ユーザ）に関するメール受信リスト６７の例を図１５に示す。この例では、送信者アドレス”ａａａ＠ｘｘｘ．ｃｏ．ｊｐ”からのメールは受信上限値６３を３０件に設定しているため、１２件全てを受信している。また、送信者アドレス”ｂｂｂ＠ｘｘｘ．ｃｏ．ｊｐ”からのメールは受信上限値６３が設定されていないため、３２件全てを受信している。これに対し、送信者アドレス”ｃｃｃ～”、”ｄｄｄ～”、”ｅｅｅ～”（いずれも未知送信者）からのメールについては、メール受信件数の合計が未知送信者メールの設定６６での受信上限値（この場合は２０件）に達したため、これ以降の未知送信者からのメールは自動削除の対象となったという状態を示している。

【００２３】メールサーバー１が以上のような設定及び処理により動作することにより、メール受信者（ユーザ）が不要と考える性質のメールについて、メール受信条件の設定により識別し、受信（つまりメールサーバー１における蓄積及び端末２への送信）を行わない。これにより、不要なメールのための無駄な電話回線４の使用及び端末２へのメール受信を回避できる。メール受信者（ユーザ）は、同一のメール送信者から設定上限値を超える件数のメールを受信することがない。スパムメールのような、何千、何万といった件数になるようなメールはメールサーバー１において未然に削除されるため、メール受信者（ユーザ）の端末２が電話回線４でメールサーバー１につなぎっ放しになってしまうというような被害を回避できる。

【００２４】また、メール自動削除設定情報６をメール受信者（ユーザ）が任意に設定することにより、メール送信者毎の細かな自動削除／受信許可の指定を行うことができる。未知のメール送信者、あるいは不明のメール送信者からのメールについても、自動削除／受信許可を指定できる。また、例えば、メール自動削除設定情報６

において特定の送信者メールアドレスを記載し、自動削除機能を有効に設定にし、受信上限値を０件とすることで、この特定の送信者からのメールを一切受け取らないようにするといったこともできる。

【００２５】更に、メールサーバー１は、受信メールを自動削除処理した場合、メール自動削除設定情報６の自動通知設定６４に基づき、削除されたメールの送信者に対して、自動削除処理した旨及び自動削除の理由などを記載したメールを自動送信する。これにより、メール送信者は、自分のメールが受信者に届かなかったことを知ることができる。

【００２６】なお、この従来技術はメールサーバー１（特にソフトウェア）のみの改良により効果を発揮できるものなので、ユーザの端末２（メール送受信用ソフトウェアを含む）を改変する必要はない。

【００２７】

【発明が解決しようとする課題】しかしながら、上記従来技術では以下のような問題点がある。第１の問題点として、メール受信者（ユーザ）が既知の個人（グループ）に関するメール受信設定を行うために、ユーザ自身がメールサーバーに送信者メールアドレス他の情報を登録処理する必要があるという点が挙げられる。ユーザによる登録処理により、必要時にすぐにメールアドレスを設定して受信を限定するなどができる。しかし、メールアドレスの登録処理には基本的に手間がかかる。また、現在の携帯電話は、上記受信設定として登録可能な件数が少なく、足りなくなることが多い。また、仮にたくさんの件数を登録可能だとしても、すべてのメールアドレス情報などを登録するための大きな手間が生じる。

【００２８】第２の問題点として、メール受信条件として同一送信者から１日に受信可能な件数の上限を設定して受信制限を行う機能の場合、例えば１日に受信する件数を１～３件のように少ない件数に設定しても、結局はその件数分が届けられてしまうことが多く、逆に件数を多く設定すると迷惑メールを防ぐことにならないなど、効果的な件数設定の仕方が難しいという点が挙げられる。

【００２９】第３の問題点として、メール受信条件としてユーザがメールアドレスを知らない未知の個人（グループ）からのメール受信を制限する機能の場合、未知のメールアドレスであっても知人や友人などからの可能性があるメールについて制限してしまう点が挙げられる。

【００３０】本発明は、かかる問題点に鑑みてなされたものであり、携帯電話のメールサーバーにおいて所定の識別条件により迷惑メール等を自動的に識別し、また、迷惑メール等について送信者メールアドレスなどの情報が変更されても上記識別条件を自動更新して識別を行い、迷惑メール等の自動削除処理を行って余計な受信を防止することのできる携帯電話のメールサーバーにおけるメール自動処分方法及びプログラムを提供することを

目的とする。

【００３１】また、ユーザが受信条件としてメールアドレスの登録処理を行うといった面倒な手間を必要とせずに、わずかな初期設定のみでシステムを利用できるメールサーバーにおけるメール自動処分方法及びプログラムを提供することを目的とする。

【００３２】

【課題を解決するための手段】かかる目的を達成するために、請求項１記載の発明は、携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にＵＲＬが含まれるかどうかを調べ、含まれる場合は抽出する抽出工程と、該工程で抽出されたＵＲＬに基づき受信メールが迷惑メールあるいはチェーンメールであるか否かの識別処理を行う識別工程と、該工程で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除処理する削除工程と、を有することを特徴としている。

【００３３】請求項２記載の発明は、請求項１記載の発明において、識別工程で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれていたＵＲＬを識別処理の際の識別条件として追加登録して識別条件を自動更新する工程をさらに有することを特徴としている。

【００３４】請求項３記載の発明は、請求項１または２に記載の発明において、抽出工程で抽出されたＵＲＬが未確認ＵＲＬである場合、該未確認ＵＲＬを本文中に含む受信メールに対する所定時間の監視処理を開始し、所定時間内は未確認ＵＲＬを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、所定時間経過後、受信件数が所定件数を超える場合、未確認ＵＲＬを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する監視工程をさらに有することを特徴としている。

【００３５】請求項４記載の発明は、請求項３記載の発明において、監視工程において、一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、未確認ＵＲＬを本文中に含むメールは迷惑メールであると判定する工程をさらに有することを特徴としている。

【００３６】請求項５記載の発明は、請求項３記載の発明において、監視工程において、一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、未確認ＵＲＬを本文中に含むメールはチェーンメールであると判定する工程をさらに有することを特徴としている。

【００３７】請求項６記載の発明は、請求項３から５のいずれか１項に記載の発明において、監視工程の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたＵＲＬを識別処理の際の識別条件として追加登録して識別条件を自動更新する工程をさらに有することを特徴としている。

【００３８】請求項７記載の発明は、請求項１から６のいずれか１項に記載の発明において、メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたＵＲＬを識別処理の際の識別条件となるＵＲＬ情報として登録して管理し、識別工程では、抽出工程で抽出されたＵＲＬについて、ＵＲＬ情報と比較し、一致する場合、受信メールを迷惑メールあるいはチェーンメールであると識別することを特徴としている。

【００３９】請求項８記載の発明は、請求項１から７のいずれか１項に記載の発明において、メールサーバーにおいて、ユーザ設定情報として、識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、受信メールについて迷惑メールあるいはチェーンメールと識別した場合、メール拒否指定の設定に基づき削除処理を実行することを特徴としている。

【００４０】請求項９記載の発明は、請求項８記載の発明において、メールサーバーにおいて、メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、ＵＲＬを本文中に含むメールに対する拒否指定であるＵＲＬメール拒否指定の３つの設定を保持し、該設定に基づき削除処理を実行することを特徴としている。

【００４１】請求項１０記載の発明は、請求項１から９のいずれか１項に記載の発明において、メールサーバーは、メールサーバーの管理者により認証を受けたＵＲＬを登録して管理し、該ＵＲＬを本文中に含む受信メールについては迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する工程を有することを特徴としている。

【００４２】請求項１１記載の発明は、携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にＵＲＬが含まれるかどうかを調べ、含まれる場合は抽出する抽出処理と、該処理で抽出されたＵＲＬに基づき受信メールが迷惑メールあるいはチェーンメールであるか否かを識別する識別処理と、該処理で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除する削除処理と、をコンピュータに実行させることを特徴としている。

【００４３】請求項１２記載の発明は、請求項１１記載の発明において、識別処理で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれるＵＲＬを識別処理の際の識別条件として追加登録して識別条件を自動更新する処理をさらにコンピュータに実行させることを特徴としている。

【００４４】請求項１３記載の発明は、請求項１１また

は１２に記載の発明において、抽出工程で抽出されたＵＲＬが未確認ＵＲＬである場合、該未確認ＵＲＬを本文中に含む受信メールに対する所定時間の監視処理を開始し、所定時間内は、未確認ＵＲＬを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、所定時間経過後、受信件数が所定件数を超える場合、未確認ＵＲＬを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する処理をコンピュータに実行させることを特徴としている。

【００４５】請求項１４記載の発明は、請求項１３記載の発明において、監視処理において、一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、未確認ＵＲＬを含むメールは迷惑メールであると判定する処理をコンピュータに実行させることを特徴としている。

【００４６】請求項１５記載の発明は、請求項１３記載の発明において、監視処理において、一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、未確認ＵＲＬを含むメールはチェーンメールであると判定する処理をコンピュータに実行させることを特徴としている。

【００４７】請求項１６記載の発明は、請求項１３から１５のいずれか１項に記載の発明において、監視処理の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたＵＲＬを識別処理の際の識別条件として追加登録して識別条件を自動更新する処理をコンピュータに実行させることを特徴としている。

【００４８】請求項１７記載の発明は、請求項１１から１６のいずれか１項に記載の発明において、メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたＵＲＬを識別処理の際の識別条件となるＵＲＬ情報として登録して管理し、識別処理では、抽出処理で抽出されたＵＲＬについて、ＵＲＬ情報と比較し、一致する場合、受信メールを迷惑メールあるいはチェーンメールであると識別する処理をコンピュータに実行させることを特徴としている。

【００４９】請求項１８記載の発明は、請求項１１から１７のいずれか１項に記載の発明において、メールサーバーにおいて、ユーザ設定情報として、識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、受信メールについて迷惑メールあるいはチェーンメールと識別した場合、メール拒否指定の設定に基づき削除処理を行う処理をコンピュータに実行させることを特徴としている。

【００５０】請求項１９記載の発明は、請求項１８記載の発明において、メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、ＵＲＬを本文中に含むメールに対する拒否指定であるＵＲＬメール拒否指定の３つの設定を保持し、該設定に基づき削除処理を行う処理をコンピュータに実行させることを特徴としている。

【００５１】請求項２０記載の発明は、請求項１１から１９のいずれか１項に記載の発明において、メールサーバーにおいて、メールサーバーの管理者により認証を受けたＵＲＬを登録管理し、該ＵＲＬを本文中に含む受信メールについては迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する処理をコンピュータに実行させることを特徴としている。

【００５２】

【発明の実施の形態】以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。図１は、本発明の実施の形態におけるメール自動処分方法及びプログラムが実行されるシステムの構成図である。本システムは、メールサーバー１、ユーザの使用する携帯電話端末２、インターネット３、電話回線４、を有する。基本的なシステム構成は従来技術と同様であり、同一の記号によって示した。

【００５３】メールサーバー１は、本発明の実施の形態におけるメール自動処分方法を実行するサーバー装置であり、このメール自動処分方法をコンピュータ処理により実現するためのプログラム（図１でのメール自動処分処理部）を含むメールサーバーソフトウェアがインストールされ、プロセッサにより実行される。インターネット３には、複数のメールサーバー１が接続され、メールの送受信処理を行う。メールサーバー１には、電話回線４を通じて複数の端末２が接続される。ここで端末２は特に携帯電話機であるので、電話回線４は、無線通信網を含む所定の通信システムで構成される。端末２は、メールを作成・送受信する機能を持つメールソフトウェアを備える。端末２がメールサーバー１に接続された状態において、端末２はメールサーバー１に蓄積されているユーザ宛のメールを取得することができる。

【００５４】図１で、メールサーバー１の備えるプログラムは、構成要素として、ｈｔｔｐフィルタ１１、迷惑メールＵＲＬ格納部１２、チェーンメールＵＲＬ格納部１３、認証ＵＲＬ格納部１４、未確認ＵＲＬ格納部１５、ユーザ用メールボックス部１６を有する。メールサーバー１は、所定のメール配送処理他の公知処理を行う。

【００５５】各格納部１２～１６は、メールサーバー１の備える記憶装置（非図示）のメモリ領域への情報の格納処理を行うモジュールであり、メモリ上に確保される各情報欄やメールボックスを管理する（後述）。ユーザ用メールボックス部１６は、ユーザ宛のメールを蓄積するメールボックスを管理し、また、当該メールシステムを利用するに当たってのユーザによる初期設定情報であるメール拒否指定情報を管理する。

【００５６】本明細書において、迷惑メールとは、同一送信者からの多数のメールを指す。チェーンメールと

は、異なる多数の送信者から送信されてくる同一内容のメールを指す。

【００５７】本方法は、メールサーバー１がユーザ宛の受信メールについてメール本文中に書かれているホームページアドレス（ＵＲＬ）をチェック対象とすることを特徴としている。ホームページアドレス（Ｗｅｂページアドレス）はＵＲＬにより記述される。ＵＲＬ（Uniform Resource Locator）とは、ネットワーク上におけるリソース指示子である。これは、例えば、"http://www.xyz.com"などの形式で記述される。"http:"は、リソースへのアクセスに用いるプロトコルの指定であり、この場合ｈｔｔｐプロトコルを用いている。"www.～"は、ネットワーク上におけるリソースのアドレス（及びパス）の一意指定である。

【００５８】本方法において、メールサーバー１は、上記のＵＲＬチェック処理を行うｈｔｔｐフィルタ１１を備える。ｈｔｔｐフィルタ１１は、インターネット３を介してメールサーバー１が受信したメールについて、メール本文にＵＲＬが含まているかどうかを調べ、含まれている場合はＵＲＬ文字列を情報として抽出する処理を行う（なお、この処理は文字列自体を抜き出す処理ではない）。本方法では、受信メール本文中から抽出したＵＲＬを識別の条件として用いて迷惑メールやチェーンメールであるかどうかを識別し、この識別の結果に応じてメールを自動処分処理するものである。

【００５９】本方法では、メールサーバー１に、ｈｔｔｐフィルタ１１によりメール本文中から抽出されたＵＲＬを格納処理する迷惑メールＵＲＬ格納部１２、チェーンメールＵＲＬ格納部１３他を設ける。各格納部１２、１３他は、抽出されたＵＲＬを使用して、受信メールが迷惑メールあるいはチェーンメールかどうかの識別処理を行う。この識別処理によって迷惑メールあるいはチェーンメールであると識別されたメールに書かれていた該当ＵＲＬは、迷惑メールＵＲＬ格納部１２、チェーンメールＵＲＬ格納部１３において保存・管理され、以後の受信メールに対する迷惑メール等であるかどうかの識別条件として使用される。この識別条件は、メール受信に伴い、随時更新される。

【００６０】メールサーバー１の各格納部１２、１３他は、受信メールについて、識別条件として格納されているＵＲＬと比較する処理を行うことにより、そのメールが迷惑メールあるいはチェーンメールあるいはその他のメールであるかを識別する。

【００６１】メールサーバー１は、メール受信時、ユーザによる受信メールについての拒否指定情報（後述）に基づき、その拒否指定で設定される拒否条件に該当する受信メールをユーザ用メールボックス部１６内のメールボックスに格納保存せず、自動削除処理する。

【００６２】このように、本方法では、受信メールについてＵＲＬを参照して迷惑メール・チェーンメール等の識別を行って該当メールを自動削除処理することによって、同一送信者から１日に受信可能なメール件数などの従来のような設定処理をする必要なくメール受信制限処理を実現する。また既知送信者以外からのメール受信の制限のための設定処理を行う必要もない。

【００６３】本方法では、ユーザ（メール受信者）は、迷惑メールやチェーンメールの受信を拒否したい場合、メールサーバー１に上述したメール拒否指定を設定する。メールサーバー１において、上記メール拒否指定の設定及びユーザ宛に届くメールは、各ユーザ毎のユーザ用メールボックス部１６内に保存・管理される。

【００６４】図６は、ユーザ用メールボックス部１６の管理する情報を示す図である。ユーザ用メールボックス部１６は、ユーザ宛のメールをユーザ端末２に送信するまで蓄積しておくメールボックスである送信ボックス１６１と、迷惑メールやチェーンメールやメール本文中にＵＲＬの書かれたメール（以下、「ＵＲＬメール」）に対する拒否指定の設定情報であるメール拒否指定情報とを管理する。メール拒否指定情報として、迷惑メール拒否指定欄１６２、チェーンメール拒否指定欄１６３、ＵＲＬメール拒否指定欄１６４を設ける。本方法では、この３つの設定欄と送信ボックスを要素とするユーザ用メールボックス部１６を設けたことも特徴としている。

【００６５】ＵＲＬメール拒否指定は、メール本文中にＵＲＬを含むメールに対する拒否であるので、これにより、迷惑メール及びチェーンメールの拒否を含む拒否指定を行うことができる。

【００６６】図７は、ユーザの端末２における、上記拒否指定を設定するための設定画面の例を示す。図７では、迷惑メール、チェーンメール、及び、ＵＲＬメールの各メールに対する拒否指定として、ＹＥＳ／ＮＯの項目をチェックすることにより設定登録が行われる。このような設定画面を介してユーザ用メールボックス部１６における各拒否指定欄１６２～１６４への設定処理が行われる。本方法では、ユーザは上記の３項目の設定のみにより迷惑メール等自動削除処理を有効とするための拒否指定の設定を行うことができる。

【００６７】図２は、迷惑メールＵＲＬ格納部１２の管理する迷惑メールＵＲＬ格納欄の構成を示す。迷惑メールＵＲＬ格納欄はいくつかのＵＲＬ格納欄から成り立っている。迷惑メールＵＲＬ格納欄には過去に当該メールサーバー１において迷惑メールであると識別されたメールに書かれていたＵＲＬ（以下、「迷惑メールＵＲＬ」）が格納される。

【００６８】図３は、チェーンメールＵＲＬ格納部１３の管理するチェーンメールＵＲＬ格納欄の構成を示す。チェーンメールＵＲＬ格納欄はいくつかの格納欄から成り立っている。チェーンメールＵＲＬ格納欄には過去に当該メールサーバー１においてチェーンメールと識別されたメールに書かれていたＵＲＬ（以下、「チェーンメ

ールＵＲＬ」）が格納される。

【００６９】メールサーバー１が受信するメールでメール本文中にＵＲＬが書かれているメールとしては、迷惑メールやチェーンメールだけではないと考えられる。例えば、メーカーやメールサーバー１の管理者からの連絡などのメールにもＵＲＬが書かれている場合がある。本方法では、メールサーバー１は、メールサーバー１の管理者等により認証を受けたＵＲＬ（以下、「認証ＵＲＬ」）を保存・管理する領域である認証ＵＲＬ格納部１４を設ける。認証ＵＲＬ格納部１４では、迷惑メール等に含まれるＵＲＬ以外の、メールサーバー１管理者により認証を受けたＵＲＬを格納する。この格納部１４により、メーカーやメールサーバー１の管理者からの連絡などのメールでＵＲＬを含むものについて、迷惑メールやチェーンメールなどと区別して受信許可することができ、このようなメールをユーザが通常通り受信することが可能となる。

【００７０】メールサーバー１は、受信メールについて、認証ＵＲＬ格納部１４の管理する認証ＵＲＬを参照し、認証ＵＲＬが書かれているメールについては迷惑メール等ではないと識別してユーザ用メールボックス部１６への格納を行う。本方法は、この認証ＵＲＬを用いた処理を行うことも特徴としている。

【００７１】次に、本方法ではまた、メールサーバー１は、受信メールについて未確認ＵＲＬの記載を発見した場合にこのＵＲＬを格納し、以後の受信メールについて監視してこの未確認ＵＲＬが記載されたメールが迷惑メール等かどうかの識別処理を行う未確認ＵＲＬ格納部１５を設ける。ここで未確認ＵＲＬとは、メール受信時点で、メールサーバー１において迷惑メールＵＲＬやチェーンメールＵＲＬあるいは認証ＵＲＬ等の情報としては登録されていないＵＲＬを指す。未確認ＵＲＬ格納部１５は、図５に参照されるような未確認ＵＲＬ確認欄を管理する。

【００７２】メールサーバー１のｈｔｔｐフィルタ１１及び未確認ＵＲＬ格納部１５は、受信メールの本文中に新しく未確認のＵＲＬを発見した場合、一旦この未確認ＵＲＬを未確認ＵＲＬ格納欄に格納し、また、この未確認ＵＲＬを含む受信メールを一時格納領域を確保して格納し、この時点以後の所定の一定時間、受信メールについて、上記未確認ＵＲＬが記載されたメールかどうかを監視処理することにより、この未確認ＵＲＬが記載されたメールが迷惑メールあるいはチェーンメールあるいはそうではない普通のメールかどうかの識別処理を行う。識別処理の結果、迷惑メールと識別した場合は、迷惑メールＵＲＬ格納部１２の格納欄に格納し、チェーンメールと識別した場合はチェーンメールＵＲＬ格納部１３の格納欄に格納し、普通のメールと識別した場合はユーザ用メールボックス部１６の送信ボックス１６１に格納する。これらにより、未確認のＵＲＬが記載されているメールに自動的に対処する。監視処理の結果、迷惑メールあるいはチェーンメールと識別されたメールについては、メール拒否指定の設定に基づき、一時格納領域に格納されている受信メールを削除処理する。

【００７３】図５は、未確認ＵＲＬ確認欄の構成を示す。未確認ＵＲＬごとに、情報領域が確保される。未確認ＵＲＬごとに、そのＵＲＬ文字列１５１、送信者メールアドレス１５２、アクセス数１５３などの情報を管理する。未確認ＵＲＬ格納部１５は、受信メールで未確認ＵＲＬが記載されたものを発見した場合、このような情報領域を確保して、その時点以後、所定の一定時間、監視処理を行う。監視処理では、一定時間内において、該当未確認ＵＲＬと同じＵＲＬが本文中に記載されたメールを受信した場合、受信メールを一時格納領域に格納して、未確認ＵＲＬ格納欄中の該当の未確認ＵＲＬ１５１の情報を更新する。その際、受信メールについて送信者メールアドレスを参照し、その送信者メールアドレス１５２ごとにレコードを設けてメール受信件数であるアクセス数１５３をカウントする。また、異なる未確認ＵＲＬを新たに抽出した場合は、次の未確認ＵＲＬ１５１情報欄を設けて格納し監視処理する。

【００７４】例えば、図５では、未確認ＵＲＬ１"www.abc.co.jp" を含んだメールとして、所定の一定時間内に、送信者"aaa@bbb.com" から２８件のメールを受信し、送信者"ccc@ddd.co.jp" から１２件のメールを受信したことを示している。

【００７５】未確認ＵＲＬ格納部１５は、上記監視処理で所定の一定時間経過後、該当未確認ＵＲＬの管理情報を参照して該当未確認ＵＲＬを含むメールが迷惑メールあるいはチェーンメールであるかどうか判定を行う。ある未確認ＵＲＬについて、ある送信者メールアドレス１５２でアクセス数１５３が所定の件数を超える場合、迷惑メールであると判定する。また、複数の送信者メールアドレス１５２があり、それらを合わせたアクセス数１５３が所定の件数を超える場合、チェーンメールであると判定する。

【００７６】メールサーバー１は、上記の処理で迷惑メールあるいはチェーンメールの含むＵＲＬであると判定された未確認ＵＲＬについて、今度は、それぞれ迷惑メールＵＲＬあるいはチェーンメールＵＲＬとして、格納部１２、１３の格納欄へそれぞれ格納し、迷惑メールあるいはチェーンメールの識別処理の際の識別条件となるＵＲＬ情報として追加登録する。各格納部１２、１３は、追加登録されたＵＲＬ情報を用いて識別処理の際の識別条件を更新し、更新された識別条件を用いてその後の識別処理を行う。

【００７７】次に、図８及び図９のフローチャートを参照して、本発明の実施の形態におけるメール自動処分方法及びプログラムを実行するメールサーバー１の動作について説明する。以下の処理の主体はメールサーバー１

である。図８で、まず、メールサーバー１は、ユーザ宛のメールをインターネット３経由で受信した場合、受信メールをｈｔｔｐフィルタ１１に通し（ステップＳ１０１）、メール本文中にＵＲＬ（ホームページアドレス）が書かれているかどうかを調べる（ステップＳ１０２）。具体的には、まず”ｈｔｔｐ”という文字列を検出し、メール本文中に”ｈｔｔｐ”文字列が含まれる場合、その”ｈｔｔｐ”文字列を含んで以後に続く文字列からなるＵＲＬ文字列について、ステップＳ１０４以後の確認処理を順に行う。ＵＲＬ文字列を含まないメールである場合、受信メールをユーザ用メールボックス部１６の送信ボックス１６１に格納する（ステップＳ１０３）。

【００７８】ＵＲＬ文字列をメール本文に含む受信メールについて、まず、迷惑メールＵＲＬ格納部１２に格納されている迷惑メールＵＲＬで一致するものがないか比較して確認する（ステップＳ１０４）。

【００７９】一致するＵＲＬがある場合（ステップＳ１０５・ＹＥＳ）、当該受信メールを迷惑メールであると判定し、次に、ユーザ用メールボックス部１６の迷惑メール拒否指定欄１６２及びＵＲＬメール拒否指定欄１６４の各拒否指定を確認し（ステップＳ１０６、Ｓ１０９）、拒否指定がなければ、送信ボックス１６１へ格納する（ステップＳ１１２）。拒否指定がある場合、各部は、当該受信メールについて、自動的な削除処理を行う（ステップＳ１０８、Ｓ１１１）。

【００８０】一致するＵＲＬはない場合（ステップＳ１０５・ＮＯ）、次に、チェーンメールＵＲＬ格納部１３に格納されているチェーンメールＵＲＬで一致するものがないか比較して確認する（ステップＳ１１３、１４）。

【００８１】一致するＵＲＬがある場合（ステップＳ１１４・ＹＥＳ）、当該受信メールをチェーンメールであると判定し、ユーザ用メールボックス部１６のチェーンメール拒否指定欄１６３及びＵＲＬメール拒否指定欄１６４の各拒否指定を確認し（ステップＳ１１５、Ｓ１１８）、拒否指定がなければ、送信ボックス１６１へ格納する（ステップＳ１２１）。拒否指定がある場合、当該受信メールについて自動的な削除処理を行う（ステップＳ１１７、Ｓ１２０）。

【００８２】一致するＵＲＬがない場合（ステップＳ１１４・ＮＯ、図８へ）、次に、認証ＵＲＬ格納部１５に格納されている認証ＵＲＬで一致するものがないかを比較して確認する（図９、ステップＳ２０１）。

【００８３】一致するＵＲＬがある場合（ステップＳ２０２・ＹＥＳ）、当該ＵＲＬを認証ＵＲＬであると判定し、送信ボックス１６１へ格納する（ステップＳ２０３）。

【００８４】一致するＵＲＬはない場合（ステップＳ２０２・ＮＯ）、当該ＵＲＬは未確認ＵＲＬであると判定し、未確認ＵＲＬ格納部１５の格納欄中にこの未確認ＵＲＬ用の情報領域を確保して格納する（ステップＳ２０４）。そして、この未確認ＵＲＬに関して、所定の一定時間の監視処理を行う（ステップＳ２０５）。この監視処理では、所定の一定時間内に当該未確認ＵＲＬと同じＵＲＬを本文中に含むメールを受信した場合に、上記確保された未確認ＵＲＬ情報領域の情報（送信者メールアドレス１５２、アクセス数１５３など）を更新する。また、別の未確認ＵＲＬが含まれたメールを受信した場合には、未確認ＵＲＬ格納欄中に別の情報領域を確保して独立した所定の一定時間の監視処理を開始する。この監視処理において、監視対象である各未確認ＵＲＬを含む受信メールについては、上記一定時間内は未確認ＵＲＬ格納部１５が確保する一時格納領域において一時蓄積する。

【００８５】未確認ＵＲＬに関して上記一定時間監視後、未確認ＵＲＬ格納欄中のアクセス数１５３等を参照し、アクセス数１５３が所定数を超える場合（ステップＳ２０６・ＹＥＳ）、この未確認ＵＲＬを含むメールは迷惑メールもしくはチェーンメールのどちらかであると識別する。

【００８６】上記のように識別された未確認ＵＲＬを含む受信メールについて、未格納ＵＲＬ確認欄中の送信者メールアドレス１５２やアクセス数１５３を参照し、同一送信者からの所定数以上のメールである場合、このＵＲＬを含むメールを迷惑メールであると判定し、このＵＲＬを迷惑メールＵＲＬとして迷惑メールＵＲＬ格納部１２に新たに登録する（ステップＳ２０９）。

【００８７】また、異なる送信者からの所定数以上のメールである場合、このＵＲＬを含むをメールをチェーンメールであると判定し、このＵＲＬをチェーンメールＵＲＬとしてチェーンメールＵＲＬ格納部１３に新たに登録する（ステップＳ２１２）。

【００８８】迷惑メールと判定した場合、ユーザ用メールボックス部１６の迷惑メール拒否指定欄１６２及びＵＲＬメール拒否指定欄１６４の拒否指定を確認し（ステップＳ２１０、Ｓ２１５）、拒否指定があれば該当受信メールを自動削除し（ステップＳ２１１、Ｓ２１７）、拒否指定がなければ送信ボックス１６１に格納する（ステップＳ２１８）。

【００８９】同様に、チェーンメールと判定した場合、ユーザ用メールボックス部１６のチェーンメール拒否指定欄１６３及びＵＲＬメール拒否指定欄１６４を確認し（ステップＳ２１３、Ｓ２１６）、拒否指定があれば該当受信メールを自動削除し（ステップＳ２１４、Ｓ２１７）、なければ送信ボックス１６１に格納する（ステップＳ２１８）。動作については以上である。

【００９０】以上により本発明の実施の形態について説明した。なお、上述した実施形態は、本発明の好適な実施形態の一例を示すものであり、本発明はそれに限定さ

れるものではなく、その要旨を逸脱しない範囲内において、種々変形実施が可能である。

【００９１】

【発明の効果】以上の説明から明らかなように、本発明によれば、携帯電話のメールサーバーにおいて受信メール本文中にＵＲＬが書かれているかどうか調べ、このＵＲＬを識別条件として用いて迷惑メール等であるか否かの識別を行うので、ＵＲＬ（ホームページアドレス）が本文中に書かれたメール（例えば、広告や勧誘としてＵＲＬを記載しているもの）について自動的に迷惑メール等の識別を行って自動処分し、ユーザの端末への受信を防止することができる。

【００９２】また、メールサーバーにおいて過去に迷惑メール等に含まれるＵＲＬであると判定されたＵＲＬを保存・管理し、これを用いて受信メールについて識別を行うことにより、瞬時にその受信メールが迷惑メール等であるかを識別することができる。

【００９３】また、この迷惑メール等識別処理のためのＵＲＬ情報はメールサーバーにおいて自動的に更新されるため、ユーザが細かな設定や再登録処理を行う必要がない。

【００９４】また、ユーザが当該メールシステムを利用するに当たって初期設定処理として必要なのは拒否指定欄における３つの設定であって手間が少なく、ユーザは面倒な登録処理をする必要がない。

【００９５】また、認証ＵＲＬ格納部を設けたことにより、メールサーバー管理者やメーカー等からの連絡のメールの本文中にＵＲＬが書かれていても、迷惑メール等との区別ができ、このようなメールについて削除処理してしまうことなく必要としているユーザに届けることができる。

【００９６】また、未確認ＵＲＬ格納部を設けたことにより、受信メールの本文中に未確認のＵＲＬが書かれていても、そのＵＲＬに関して迷惑メール等であるかの識別ができ、自動処分や蓄積等の対応処理を行うことができる。迷惑メール等の送信者が送信元メールアドレスを変更したり、本文中のＵＲＬを変更したメールを送信してくる場合にも対応できる。

【図面の簡単な説明】

【図１】本発明の実施の形態における迷惑メール自動処分方法及びプログラムを実行するシステムの基本構成図である。

【図２】迷惑メールＵＲＬ格納欄の構成図である。

【図３】チェーンメールＵＲＬ格納欄の構成図である

【図４】認証ＵＲＬ格納欄の構成図である。

【図５】未確認ＵＲＬ格納欄の構成図である

【図６】ユーザ用メールボックス部１６の管理情報の構成図である。

【図７】ユーザの端末２における、各拒否指定の設定画面の例である。

【図８】本発明の実施の形態における迷惑メール自動処分方法及びプログラムの動作を示すフローチャートである。

【図９】本発明の実施の形態における迷惑メール自動処分方法及びプログラムの動作を示すフローチャート（図８の続き）である。

【図１０】従来技術のシステムの基本構成図である。

【図１１】従来技術のメールサーバー１における迷惑メール自動処分方法で用いられるメール受信条件情報５の構成図である。

【図１２】従来技術のメールサーバー１におけるメール自動削除設定情報６の構成図である。

【図１３】従来技術のシステムにおけるメールの送受信の様子を示す図である。

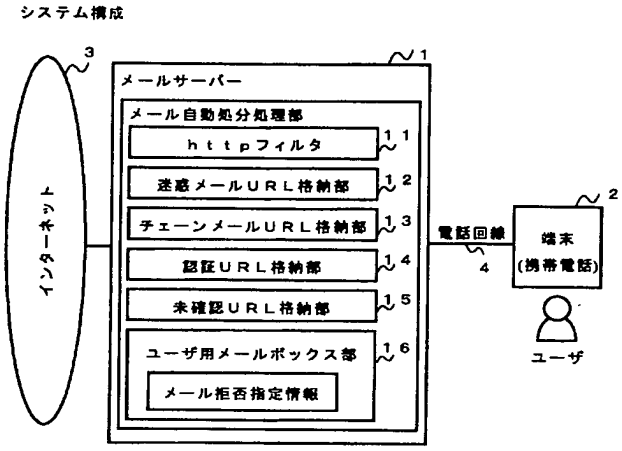
【図１４】メール自動削除の設定例である。

【図１５】メール受信リスト６７の例である。

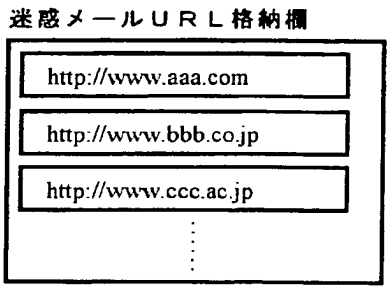
【符号の説明】

１　メールサーバー
２　ユーザの携帯電話端末
３　インターネット
４　電話回線
１１　ｈｔｔｐフィルタ
１２　迷惑メールＵＲＬ格納部
１３　チェーンメールＵＲＬ格納部
１４　認証ＵＲＬ格納部
１５　未確認ＵＲＬ格納部
１６　ユーザ用メールボックス部
１５１　未確認ＵＲＬ
１５２　送信者メールアドレス
１５３　アクセス数
１６１　送信ボックス
１６２　迷惑メール拒否指定欄
１６３　チェーンメール拒否指定欄
１６４　ＵＲＬメール拒否指定欄
５　メール受信条件情報（従来技術）
６　メール自動削除設定情報（従来技術）
７　メール送信者及び送信者端末
８　送信側メールサーバー
５１　同一送信者条件
５２　最大サイズ条件
５３　既知送信者リスト
６１　送信者メールアドレス
６２　自動削除対象の設定情報
６３　受信可能メール件数の上限値
６４　削除通知設定
６５　送信者不明メールの設定
６６　送信者未知メールの設定
６７　メール受信リスト
６８　日単位・送信者単位でのメール受信件数

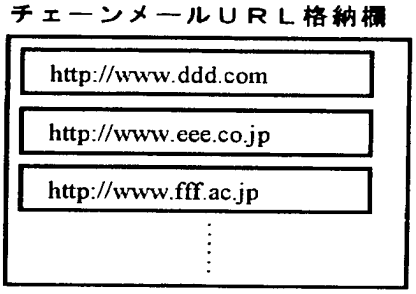
【図１】



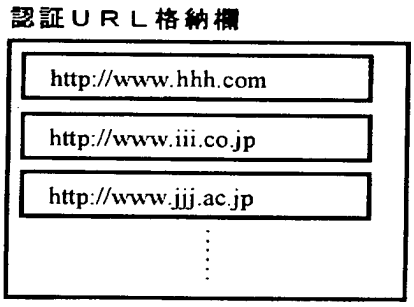
【図２】



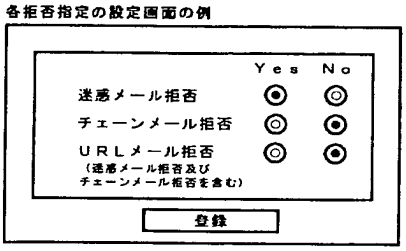
【図３】



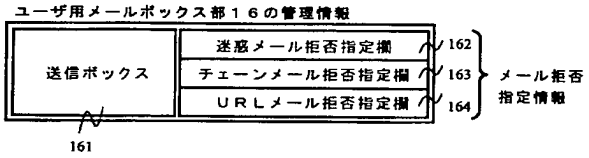
【図４】



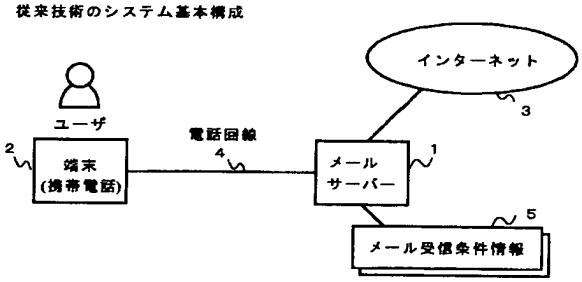
【図７】



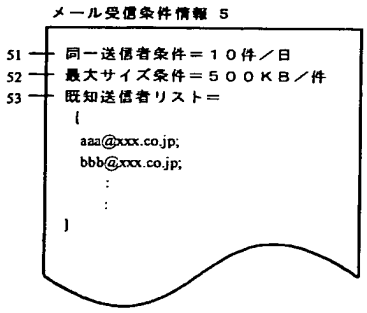
【図６】



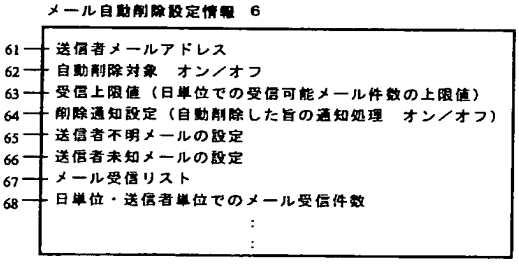
【図１０】



【図１１】



【図１２】



【図５】

未確認ＵＲＬ格納欄

未確認ＵＲＬ１　http://www.abc.co.jp　151

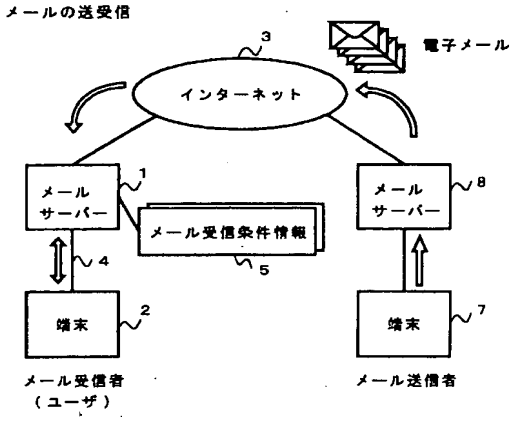
送信者メールアドレス	アクセス数
aaa@bbb.com	28
ccc@ddd.co.jp	12
・・・	・・・

152　153

未確認ＵＲＬ２　http://www.def.com

送信者メールアドレス	アクセス数
xxx@yyy.com	10
zzz@uuu.co.jp	36
www@aaa.com	3
・・・	・・・

【図１３】



【図１４】

メール自動削除の設定例

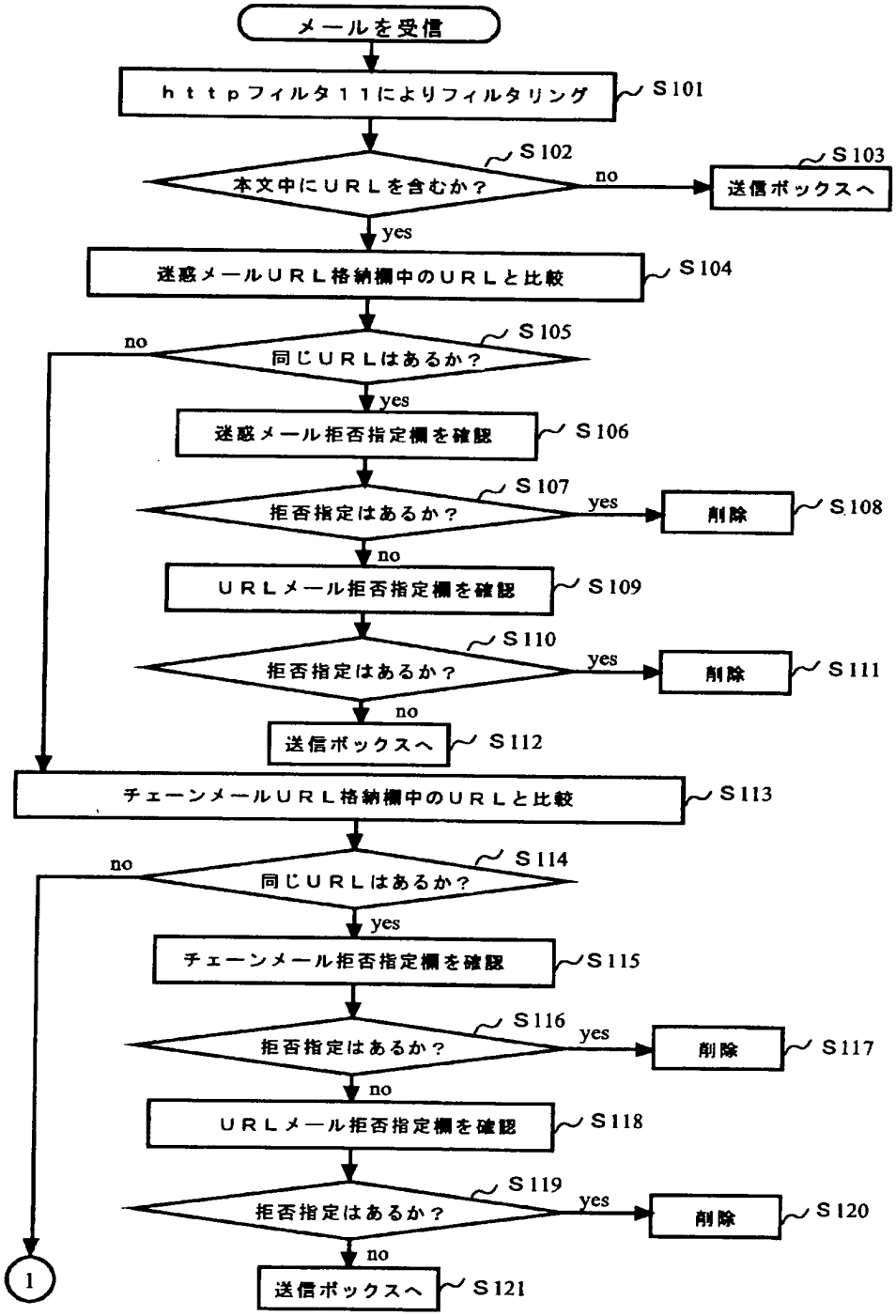
送信者メールアドレス	自動削除	受信上限値	自動通知
不明送信者	する	０件	しない
未知送信者	する	２０件	する
ａａａ@ｘｘｘ．ｃｏ．ｊｐ	する	３０件	する
ｂｂｂ@ｘｘｘ．ｃｏ．ｊｐ	しない	－	－

【図１５】

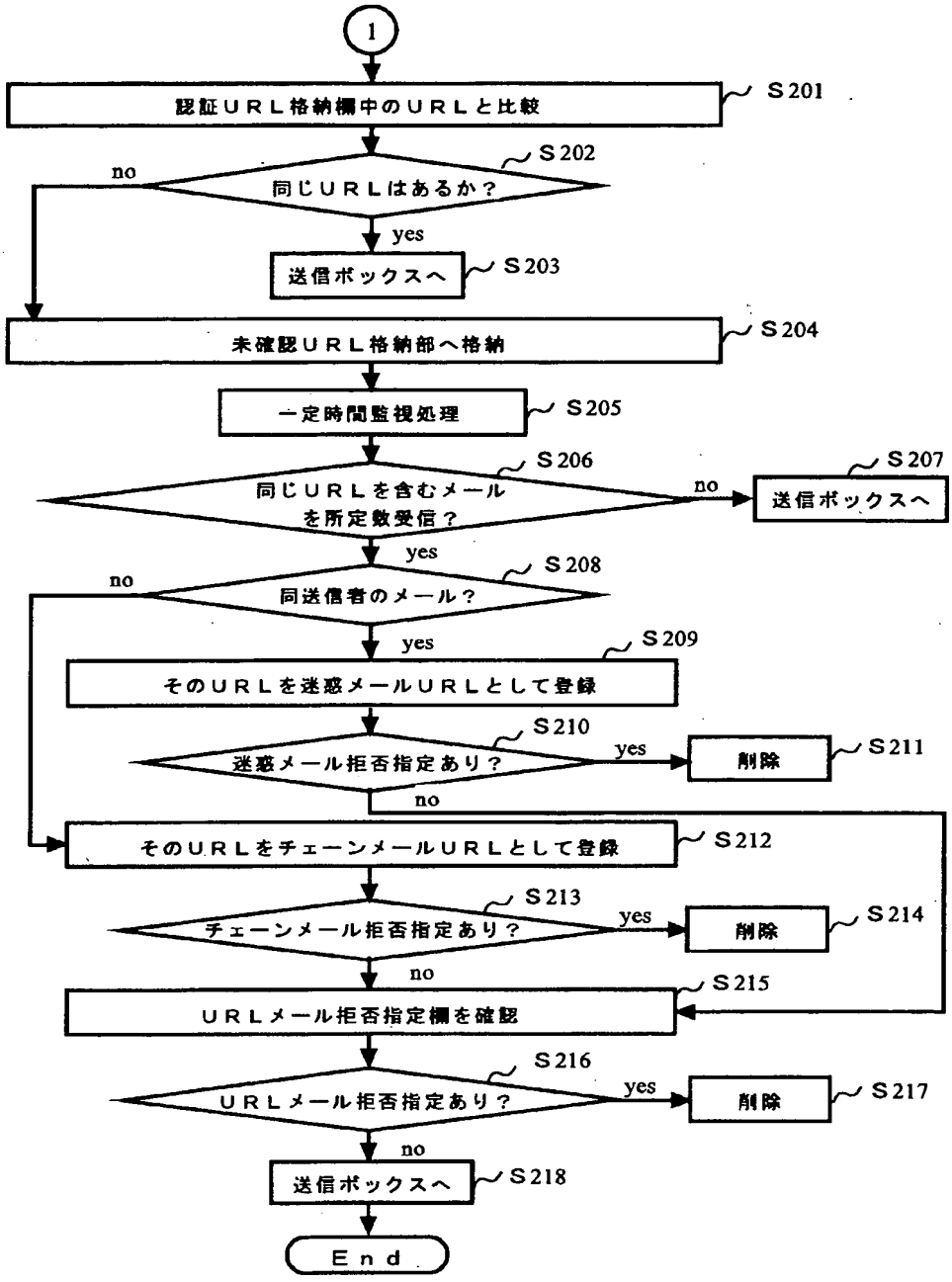
メール受信リスト６７の例

送信者メールアドレス	本日の件数	（備考）
不明送信者	０件	
ａａａ@ｘｘｘ．ｃｏ．ｊｐ	１２件	
ｂｂｂ@ｘｘｘ．ｃｏ．ｊｐ	３２件	
ｃｃｃ@ｘｘｘ．ｃｏ．ｊｐ	８件	（未知送信者）
ｄｄｄ@ｘｘｘ．ｃｏ．ｊｐ	１０件	（未知送信者）
ｅｅｅ@ｘｘｘ．ｃｏ．ｊｐ	２件	（未知送信者）

【図８】


メールを受信
ｈｔｔｐフィルタ１１によりフィルタリング
S101
本文中にＵＲＬを含むか？
S102
no
送信ボックスへ
S103
yes
迷惑メールＵＲＬ格納欄中のＵＲＬと比較
S104
同じＵＲＬはあるか？
S105
no
yes
迷惑メール拒否指定欄を確認
S106
拒否指定はあるか？
S107
yes
削除
S108
no
ＵＲＬメール拒否指定欄を確認
S109
拒否指定はあるか？
S110
yes
削除
S111
no
送信ボックスへ
S112
チェーンメールＵＲＬ格納欄中のＵＲＬと比較
S113
同じＵＲＬはあるか？
S114
no
yes
チェーンメール拒否指定欄を確認
S115
拒否指定はあるか？
S116
yes
削除
S117
no
ＵＲＬメール拒否指定欄を確認
S118
拒否指定はあるか？
S119
yes
削除
S120
no
送信ボックスへ
S121
1

【図９】


1
認証ＵＲＬ格納欄中のＵＲＬと比較
S201
同じＵＲＬはあるか？
S202
no
yes
送信ボックスへ
S203
未確認ＵＲＬ格納部へ格納
S204
一定時間監視処理
S205
同じＵＲＬを含むメール
を所定数受信？
S206
no
送信ボックスへ
S207
yes
同送信者のメール？
S208
no
yes
そのＵＲＬを迷惑メールＵＲＬとして登録
S209
迷惑メール拒否指定あり？
S210
yes
削除
S211
no
そのＵＲＬをチェーンメールＵＲＬとして登録
S212
チェーンメール拒否指定あり？
S213
yes
削除
S214
no
ＵＲＬメール拒否指定欄を確認
S215
ＵＲＬメール拒否指定あり？
S216
yes
削除
S217
no
送信ボックスへ
S218
End